AO 106 (Rev. 04/10) Application for a Search Warrant

AUSA reviewed: J. McAlister

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

4 CHELSEA BOULEVARD, APARTMENT # 606, HOUSTON, TEXAS 77066

Case No. H19-0924M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

4 CHELSEA BOULEVARD, APARTMENT # 606, HOUSTON, TEXAS 770, which is further described in Attachment A.

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized):*

Please see Attachment B which is made a part of this Application

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C.Section 1343 & 1349	Wire Fraud & Conspiracy
18 U.S.C.Section 1956	Money Laundering

The application is based on these facts:
Please see the attached Affidavit, which is made a part of this Application.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DHS Special Agent Darren R. Rusakiewicz
Printed name and title

Sworn to before me and signed in my presence.

Date: 5-21-19

Judge's signature

City and state: Houston, Texas

Nancy K. Johnson United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF THE RESIDENCE/PREMISES AND OUT BUILDING(S) LOCATED AT: **4 CHELSEA BOULEVARD** **APARTMENT # 606** **HOUSTON, TX 77066**	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Darren R. Rusakiewicz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **4 CHELSEA BOULEVARD, APARTMENT # 606, HOUSTON, TEXAS 77066**, hereinafter "**TARGET LOCATION**," further described in Attachment A, for the things described in Attachment B.

2. I am currently employed by the U.S. Department of Homeland Security (DHS), Homeland Security Investigations. I have been a Special Agent with Homeland Security Investigations (HSI) since March 2009 and am currently assigned to the Document and Benefit Fraud Task Force. Prior to employment with HSI, I was an Officer with the United States Secret Service Uniformed Division (USSS/UD). I have attended and completed the Criminal Investigator Training Program at Glynco, GA, as well as academies for HSI and USSS/UD. I have personally conducted and participated in numerous investigations involving criminal activity including but not limited to controlled substance offenses, firearms violations, money laundering (including international money laundering), bulk cash smuggling, structuring, benefit fraud, credit card fraud, and identity theft. I have also authored and/or executed numerous

search and seizure warrants relating to money laundering, structuring, bank fraud, check fraud, credit card fraud, bank fraud, wire fraud, and identity theft.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have set forth only the facts that I believe are necessary to establish probable cause that violations of 18 U.S.C. § 1956 (Money Laundering and Money Laundering Conspiracy) and 18 U.S.C §§ 1343, 1349 (Wire Fraud and Wire Fraud Conspiracy) have been committed.

PROBABLE CAUSE

Business Email Compromise and Other Fraud Schemes

4. Business Email Compromise (BEC) Schemes are sophisticated scams conducted by organized fraud rings which target businesses and other entities in the financial sector which regularly perform wire transfers or other money transfers. The fraud rings recruit co-conspirators to open and manage bank accounts for the sole purpose of receiving fraudulent wire transfers. These bank accounts are referred to as "drop" accounts.

5. Once these "drop" accounts have been opened, victims are targeted with false wiring instructions sent to their email accounts from spoofed email accounts. The victims are then instructed to send large wire transfers into the "drop" accounts.

6. After the wire transfers have entered the "drop" accounts, the funds are quickly depleted. The most common methods of depletion are the purchase of cashier's checks, wire transfers to account holders in foreign countries, and cash withdrawals.

7. Based upon my training and your affiant is aware that fraudulent actors typically do not exclusively involve themselves in only one type fraud schemes. In most cases these fraudulent actors will involve themselves in any fraud scheme in which they can easily obtain fraudulent funds, and will be engaged in multiple fraud schemes at the same time. These type of fraudulent schemes frequently are Romance Fraud, Online Sales Fraud (advertising for the sale of puppies or bird that don't exist), counterfeit check fraud, and fraudulent income tax refund fraud.

Summary of Investigation by HSI Baltimore

8. In June 2017, HSI Baltimore began an investigation into a Business Email Compromise fraud ring run by Aldrin FOMUKONG. On December 18, 2017, FOMUKONG and other co-conspirators to include Carlson CHO, Izou-Ere DIGIFA, and Yanick EYONG, were indicted by a Grand Jury empaneled in the District of Maryland for Conspiracy to Commit Money Laundering, 18 U.S.C. § 1956(h). FOMUKONG and another co-conspirator were also indicted for Conspiracy to Commit Wire Fraud, 18 U.S.C. § 1349. Criminal No. PWG-17-661. The conspiracies charged ranged from in or about February 2016 through in or about July 2017.

9. As part of the continuing investigation into FOMUKONG and others, law enforcement has identified JASON RAPHEAL NANA CHINJI and JOEL MUKONG as being part of the Business Email Compromise fraud ring run by FOMUKONG. On May 20, 2019, CHINJI and MUKONG were indicted by a Grand Jury empaneled in the District of Maryland for Conspiracy to Commit Money Laundering, 18 U.S.C. § 1956(h). Criminal No. PWG-19-243 (under seal).

10. The roles of MUKONG and CHINJI within the money laundering conspiracy were to recruit individuals in the Houston, Texas area to register fictitious businesses with the Harris County, Texas County Clerk. Once the businesses were registered, MUKONG and CHINJI would

provide the names of the businesses to FOMUKONG. FOMUKONG would wait until a fraudulent wire transfer had entered a drop account controlled by him, and then instruct the holder of the drop account to purchase a large denomination cashier's check made out to the business name given to him by MUKONG and CHINJI.

11. Once the cashier's check was obtained, either FOMUKONG and/or a co-conspirator would fly to Houston, Texas, where they would meet with MUKONG and CHINJI. MUKONG and CHINJI would then have the fictitious Texas business registrant cash the cashier's check at a local check cashing store. MUKONG and CHINJI would then receive a percentage of the proceeds of the cashier's check from FOMUKONG.

12. In the paragraphs below, your affiant will list specific instances in which CHINJI and MUKONG participated in the fraud scheme with FOMUKONG and others. These instances are set forth to establish probable cause and do not constitute all of the evidence your affiant has obtained regarding CHINJI and MUKONG.

Mercatel Investment

13. On May 22, 2017 the business MERCATEL INVESTMENT LLC was registered in the state of Maryland by Izou-Ere DIGIFA. On May 23, 2017, DIGIFA also opened a SunTrust bank account ending in 4431 in the name of MERCATEL INVESTMENT LLC ("SunTrust x4431").

14. On June 7, 2017, SunTrust x4431 received an incoming wire transfer in the amount of $50,703. Law Enforcement subsequently learned that the sender of the wire transfer (Victim 1) was a company in Colorado that had reported being a victim of a BEC scheme.

15. On June 9, 2017, DIGIFA purchased SunTrust official check No. 4681041315 in the amount of $39,486 made out to SQT6 SOLUTION CO. DIGIFA gave the check to

FOMUKONG, who then traveled to Houston, Texas, where he met with MUKONG and CHINJI. The check was then deposited into a Capital One bank account ending in 6452 ("Capital One x6452"). Investigators received information from Capital One that Capital One x6452 had been opened by Individual 1.

Fonanjei Trading

16. On June 7, 2017, Frankline FONANJEI opened a Bank of America account ending in 7760 in the name of FRANKLINE FONANJEI SOLE PROP DBA FONANJEI TRADING at the Bank of America branch in Marlborough, Massachusetts ("BOA x7760"). The account had minimal activity until June 15, 2017 when it received an incoming wire transfer in the amount of $227,000 from a Bank of America account belonging to Victim 2. Victim 2 told law enforcement that he was attempting to purchase a home in California, and was trying to send $227,000 to a Title Company in California to complete the purchase. He had unknowingly received false wiring instructions via email which resulted in him sending a false wire transfer in the amount of $227,000 to BOA x7760 on June 15, 2017. After the wire transfer entered the account, FONANJEI conducted several transactions including the purchase of Bank of America Cashier's Check No. 1068905338 in the amount of $90,000 and Bank of America Cashier's Check No. 1242008361 in the amount of $95,000. Both checks were purchased in the Dallas, Texas area on June 16, 2017 and made out to SQT6 SOLUTION CO.

17. Both cashier's checks were negotiated at Senor Check Cashing stores in Houston, Texas. The checks were endorsed with Individual 1's name on them.

18. During an interview with law enforcement, FONANJEI stated that he had been recruited to open BOA x7760 by Carlson CHO. FONANJEI said that after the wire transfer

entered the account, CHO told him they had to go to Texas because CHO knew someone who could cash checks[1].

19. FONANJEI said he then flew to Dallas, Texas with CHO, where they purchased the cashier's checks listed above. They then flew to Houston, Texas. Once in Houston, Texas, FONANJEI and CHO met two individuals and gave them the cashier's checks. FONANJEI then identified photographs of CHINJI and MUKONG as the two individuals that he met with in the hotel. FONANJEI also stated that he saw FOMUKONG at the hotel but did not interact with him.

Interview of Individual 1

20. Law Enforcement also interviewed Individual 1 as part of this investigation. Individual 1 told investigators that in 2017 she was living at an extended stay motel in Houston, Texas when she was approached by two African males that drove a red Dodge Challenger[2]. Individual 1 said she knew them as "Mike" and "Mike's brother."

21. Individual 1 said that "MIKE" told her he would pay her to open bank accounts and businesses in names that he would give her. Individual 1 agreed and rode with "Mike" and "Mike's brother" to the Harris County, Texas Clerk's office where she registered the business SQT6 SOLUTION CO. Individual 1 said she was also driven to a Capital One Bank branch where she opened an account in the name of SQT6 SOLUTION CO. After opening the bank account she gave all of the paperwork and debit cards to "Mike" and "Mike's brother".

---

[1] Your affiant has reviewed text messages between FOMUKONG and CHO in which FOMUKONG instructed CHO to fly to HOUSTON and provided him with phone numbers for CHINJI.

[2] Individual 1 referred to the vehicle as both a Dodge Challenger and a Dodge Charger. Your affiant has reviewed photographs on phones seized from FOMUKONG. Several of the photographs show FOMUKONG and MUKONG in the parking lot of an apartment complex with a red Dodge Challenger behind them. These photographs were also shown to Individual 1 and she stated that was the car driven by "Mike's brother".

22. Individual 1 was shown a copy of SunTrust official check No. 4681041315. Individual 1 said that she thought the check was deposited into her account by either "Mike" or his brother at an ATM.

23. With regards to the two Bank of America Cashier's checks referenced above, Individual 1 remembered trying to negotiate a large cashier's check in the name of SQT6 SOLUTION CO. at a check cashing location in Houston, Texas. Individual 1 stated that the employee at the check cashing business told her the check was fraudulent and wouldn't cash it. Individual 1 stated she gave the check back to "Mike" and his brother.

24. Individual 1 was shown photographs of CHINJI and MUKONG and identified CHINJI as being the person she knew as "Mike" and MUKONG as being the person she knew as "Mike's brother".

25. Individual 1 was also shown a picture of Individual 2. Individual 1 stated that she knew Individual 2 as "ASHTON" and that in 2017 he lived in the same extended stay motel that she was living in. Individual 1 also said that she knew that Individual 2 did "business" with CHINJI and MUKONG. Individual 1 clarified that "business" meant registering businesses and opening bank accounts.

CL Escrow – Individual 2

26. On June 15, 2017, Yanick EYONG registered the business CL ESCROW LLC with the state of Maryland. EYONG then opened a Bank of America account ending in 0042 ("BOA x0042") in the name of CL ESCROW LLC on June 17, 2017.

27. On June 21, 2017, BOA x0042 received an incoming wire transfer in the amount of $6,000,000 from Victim 3, a company in Boston, Massachusetts. Victim 3 informed law

enforcement that they had been the victim of a BEC scheme which had caused them to send the wire transfer.

28. On June 23, 2017, EYONG obtained three separate Bank of America cashier's checks in the amount of $95,000 each and made out to QPZYTX LINK CO. All three of these checks were negotiated at Senor Check Cashing in Houston, Texas on June 26, 2017 by Individual 2.

29. Information received from the Harris County, Texas Clerk showed that QPZYTX LINK CO was registered by Individual 2 on May 24, 2017.

30. During an interview with law enforcement, Individual 2 stated that in 2017 he was living in an extended stay motel in Houston, Texas where he met an African Male with a French/African accent he knew as "Mike". Mike was accompanied by another black male that Individual 2 described as a "quiet guy".

31. "Mike" gave him the name of QPZYTX LINK CO and drove him to the Harris County, Texas Clerk's office where he registered it. "Mike" and the "quiet guy" also drove him to a check cashing location in the Houston, Texas area where he negotiated multiple cashier's checks in the name of QPZYTX LINK CO.

WhatsApp Communications

32. As part of the investigation, investigators seized phones belonging to FOMUKONG and conducted forensic examinations on them. The examination showed that FOMUKONG used the chat application WhatsApp to communicate with co-conspirators both in the United States and South Africa in furtherance of the fraud scheme.

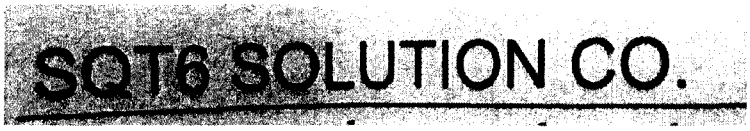
33. Your affiant reviewed a group chat string between FOMUKONG and the phone numbers 405-400-5251 and 312-522-0446. Phone number 405-400-5251 was listed in

FOMUKONG's phone as Tebeng and 312-522-0446 was listed as Nana Payee Buzic. Subscriber records showed that 405-400-5251 was a T-Mobile phone number registered to Joel MUKONG. FOMUKONG previously provided 312-522-0446 as "Jason's" phone number. Based on my knowledge of the investigation, training, and experience, I know that phone number 405-400-5251 was utilized by MUKONG and the phone number 312-522-0446 was utilized by CHINJI.

34. Your affiant reviewed the chat string and noted the following relevant chats between FOMUKONG, CHINJI, and MUKONG:

6/16/17

Mukong:

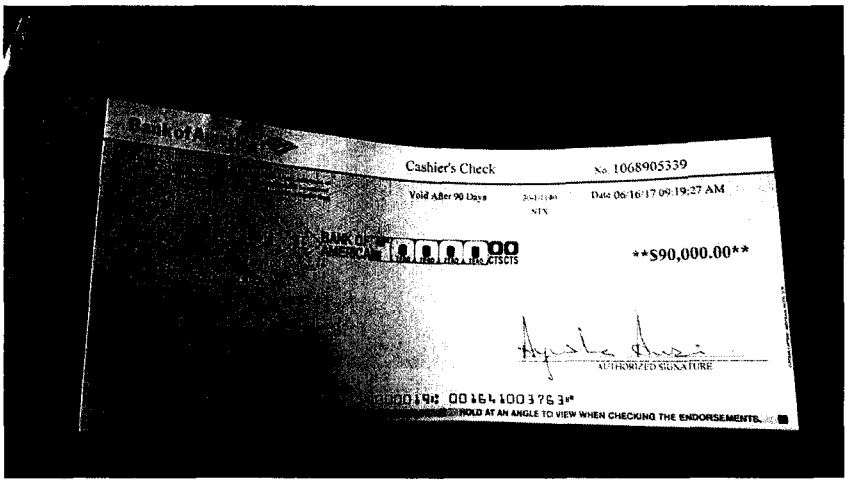


Fomukong: Kfrm

Fomukong: SQT6 Solution CO

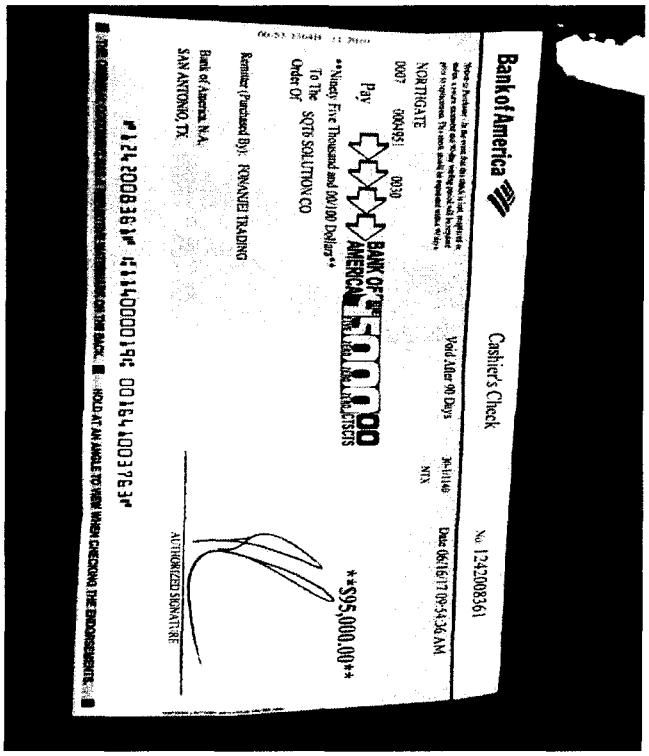
Mukong: Yup

Fomukong: K

Fomukong: 

Mukong: Kfrim

Mukong: Albanky don dowam gain

Fomukong: 

6/21/17

Mukong: Qpzytx link co

Fomukong: CAllme

Fomukong: Nana

6/23/17

Fomukong: Qpzytx link co

Fomukong: Na dis one right

Fomukong: Make ie de under

Chinji: Just do all for de

Chinji: NJo use the name again

Chinji: Are mean the personal name

Chinji: Do all under the Qpzytx link co

35. Based upon my training and experience, your affiant believes that on June 16, 2017, when MUKONG sent FOMUKONG the picture of SQT6 Solutions Co, it was to instruct FOMUKONG to get cashier's checks payable to that name in relation to the Fonanjei Trading BEC scheme described above, and that FOMUKONG then sends photos of the cashier's checks to CHINJI and MUKONG.

36. Your affiant also believes that when MUKONG and CHINJI are talking about Qpzytx link co on June 21, 2017 and June 23, 2017, they are instructing FOMUKONG on how to purchase the cashier's checks referenced above in relation to the CL Escrow BEC scheme.

DHS-OIG Investigation of Joel MUKONG

37. On February 20, 2019, an investigator with the United States Attorney's Office in Houston, Texas contacted a Special Agent, Department of Homeland Security, Office of Inspector General, to report an online puppy sale scam in which victims wired deposits to a Houston area man who was advertising purebred puppies for sale on a number of websites. At least two of these websites had used the investigator's home address in place of the breeder's address, which led to victims of the scam contacting the investigator when the puppies they had paid for were not delivered. Victims relayed that the fraudulent breeder identified himself as Demeris HILL.

38. One of these websites, www.starchowchows.com, was registered anonymously on January 25, 2019. On February 12, 2019, an elderly female from Hawaii arranged to purchase a Chow puppy from HILL through the website. The victim, who sent HILL $1,425 via wire transfer, gave Investigators a copy of the wire transfer request form that identified a Comerica Bank account in HILL's name. Comerica Bank provided Investigators with bank security footage that showed two black males making cash counter and ATM withdrawals from the same account between

January 18, 2019 and February 13, 2019. Investigators compared the images to HILL's Texas driver's license and positively identified HILL making a cash withdrawal from the account at a Houston area Comerica Bank on January 18, 2019.

39. Investigators reviewed the Federal Trade Commission (FTC) Consumer Sentinel database to identify additional victims who attempted to purchase puppies from HILL. One such victim provided investigators with images of his Bank of America account that showed a Zelle wire transfer in the amount of $650 from the victim to HILL's Comerica Bank account on January 27, 2018. Comerica Bank images showed the second black male making cash withdrawals from the same account the morning after the victim wired the money to HILL.

40. Investigators reviewed Southwest Border Transaction Record Analysis Center (TRAC) records to identify recent overseas wire transfers made by HILL. On January 2, 2019, HILL initiated a Western Union wire transfer in the amount of $720 from Houston to a Cameroon National residing in Hangzhou, China named Charllotte Oyere AYUK. On January 7, 2018 a second individual named Joel MUKONG using Texas driver's license 43025124 sent a Western Union wire transfer in the amount of $1950 from a Western Union location in Houston to AYUK. Investigators compared MUKONG's Texas driver's license to images provided by Comerica Bank and identified MUKONG as the same individual making multiple ATM withdrawals from the HILL Comerica Bank account from Houston area ATMs on January 28, 2019.

41. Investigators subsequently reviewed multiple complaints on consumer advocacy website www.reportscam.com that identified an individual named Joel MUKONG as the perpetrator of fraudulent puppy sales through a website called www.starretrievers.com.

Residence to be Searched

42. Law Enforcement received information from the Carter Museum District Apartments located at 4 Chelsea Boulevard, Houston, TX 77006. Lease records indicate that MUKONG moved into Apartment # 606 on or about January 8, 2019 and is currently still a leaseholder.

43. On May 17, 2019, law enforcement conducted surveillance at the Carter Museum District Apartments. At approximately 6:45 am, an individual matching the description of CHINJI was observed walking two small dogs outside of the building. At approximately 7:00 am, law enforcement observed a green Mini Cooper automobile registered to Joel MUKONG parked in the parking garage for the Carter Museum District Apartments.

44. From my training and experience and knowledge gained investigating this and other fraud schemes, your affiant is aware that criminals (just like non-criminals) frequently maintain and store current and old cellular telephones and computers within their residences.

45. In addition, from my training and experience and knowledge gained investigating this and other fraud schemes, once a member of a fraud has established a WhatsApp or other chat messenger application account using a specific phone number, in most cases they never change the phone number that is utilized with the original account. The perpetrators of the fraud may switch the handset, or the actual physical cell phone that is being used, but the chat application account remains unchanged and is typically transferred (along with the chats and other data) to the new cellular phone. In addition, your affiant knows that in many cases the perpetrators feel confident that by using the chap application WhatsApp their communications between other members of the fraud scheme will avoid detection from law enforcement. As such, your affiant is aware that many times these fraudulent actors do not feel the need to dispose of previously used

cellular telephones for the purpose of avoiding detection by law enforcement and simply store the previously used cellular phones in their residence.

46. Your affiant is aware from prior experience that members of BEC fraud schemes, and this BEC fraud scheme in particular, frequently accomplish this need for communication through the use of third-party messaging applications, such as WhatsApp and Facebook Messenger, which are stored on electronic devices. Members of fraud schemes also employ these third-party messaging applications in part to avoid law enforcement detection. WhatsApp uses end-to-end encryption and Facebook Messenger can be set to use end-to-end encryption. As a result, the messages being sent between members of the fraud scheme cannot be intercepted, and will only reside in an unencrypted form on the actual devices from which they were sent or received.

47. Your affiant is aware from prior experience reviewing the contents of electronic devices utilized by individuals in this case and reviewing other cases in which electronic devices were utilized, which were lawfully searched (via consent or a search warrant) has led to valuable evidence. Based on these search warrants of electronic devices, your affiant is aware that law enforcement officers were able to obtain valuable evidence of fraud schemes and criminal wrongdoing throughout the various components held within a cellular phone and/or computer including, but not limited to, call logs, contact lists, text messages, GPS locations, photos, videos, applications, documents, e-mails, and notes.

48. Your affiant is also aware, from prior experience, that analysis of the names and telephone numbers contained in cellular telephones as well as sent and received text messages is very useful to law enforcement and provides valuable evidence concerning the scope of the contact on cellular telephones. In addition to the ability to store names and numbers, many cellular

telephones have the technical capability to store email, text messages, photos, IP addresses and voice recordings, browse internet websites, and utilize GPS features, which have also proven to be valuable information for law enforcement.

49. Based on your affiant's training and experience as a special agent with HSI, the investigation to date, and previous investigations and searches, as well as common knowledge, your affiant further believes criminals (just like non-criminals) maintain records regarding bank accounts, real property records, business records, and tax records at their residences. Such records would include banking institutions and account numbers, bank account signature cards and account opening documentation, bank statements, check books and cancelled checks, account deposits and offsets, paperwork regarding safe deposit boxes established and/or maintained, paperwork and passwords pertaining to electronic banking for domestic and offshore bank accounts, real estate purchases, sales, and general records, utility documents, deeds, titles, investment properties, income, and expenses, real estate tax documents, vehicle purchase, sale, or maintenance records, business and/or trust records, agreements, contracts, client listings, domestic and international business transactions, business tax returns and related tax documents, individual income tax returns and related tax documents, mailings to/from the IRS, state, or local taxation entities, and other tax-related records and/or correspondence further described as items to be searched for in Attachment B.

50. Your affiant also knows that criminals often withdraw funds from bank accounts tied to their fraudulent conduct in order to attempt to conceal the funds in the form of cash or cash equivalents. Based on my training and experience, your affiant also knows that criminals often store the fraudulently obtained cash or cash equivalents in concealed locations within their residence.

51. As set forth in this affidavit, investigators believe JOEL MUKONG to be a member of ALDRIN FOMUKONG'S fraud scheme. Based upon my training and experience, and knowledge of these fraud schemes, I believe that JOEL MUKONG is concealing evidence of his criminal violations, as well as the fruits and instrumentalities of these violations, in the **TARGET LOCATION**.

SEARCH OF ELCTRONIC INFORMATION

52. As described in Attachments A and B, this application seeks permission to search and seize items that might be found in the **TARGET LOCATION** in whatever form they are found. Your affiant submits that if a computer or electronic medium is found on the premises, there is probable cause to believe relevant records and communications will be stored in that computer or electronic medium.

53. Cellular telephones, personal digital assistants (PDAs), smart phones, and tablets are computer-type devices capable of creating, storing, and transmitting electronic data and are believed to contain some of the evidence described in the warrant. For example, most of these devices can contain address books, correspondence in the form of e-mails and text messages, electronic receipts, photographs that may identify assets and associates, and other documents found on computers and in paper form. Because of the vast number of different devices on the market, and the complexity of analyzing some of the devices, I hereby request the Court's permission to seize these or similar devices and to "image" or analyze the device(s) off-site.

54. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only the devices (the "storage medium") that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There

is probable cause to believe that this forensic electronic evidence will be on the devices identified in Attachment B in the **TARGET LOCATION** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely

accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, electronic devices typically contain information that log: user account session times and durations, activity associated with user accounts, and the IP addresses through which the device accessed networks and the internet. Such information allows investigators to understand the chronological context of electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a device may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media. The geographic and timeline information described herein may either inculpate or exculpate the device user. Last, information stored within a device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within the device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a storage medium works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

54. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans or downloads of the entire medium, using a tool such as Cellebrite, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

55. For the above-stated reasons, your affiant respectfully requests that search and seizure warrants be issued for the premises described in Attachments A, for items and information further described in Attachment B.

Respectfully submitted,

Special Agent Darren R. Rusakiewicz
Homeland Security Investigations

Sworn to before me this 21 day of May, 2019 and I find probable cause.

Nancy K. Johnson
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

The property to be searched is the residence located at 4 CHELSEA BOULEVARD, APARTMENT # 606, HOUSTON, TX 77066. The property is further described as a multi-level commercial apartment building.

ATTACHMENT B
Particular Things to be Seized

1. All records relating to violations of wire fraud and wire fraud conspiracy (18 U.S.C. §§ 1343 and 1349) and money laundering and money laundering conspiracy (18 U.S.C. § 1956), those violations involving JOEL MUKONG, RAPHAEL JASON NANA CHINJI, ALDRIN FOMUKONG, and others, and occurring after January 1, 2016, including:

a. All financial documents, records, and property, including bank records, loan records, credit card records, ledgers, checks or other monetary instruments, check registers, bank statements, credit cards, lines of credit, safe deposit box keys and records, deposit records, faxes, memoranda, correspondence, applications, telephone records, and other documents;

b. Records relating to federal, state, and local tax returns.

c. Identity documents including, but not limited to, U.S. and foreign passports, visas, I-94 Departure Records, birth certificates, social security cards, and foreign national identity documents.

d. Documents reflecting the acquisition, purchase, or ownership of assets, including titles, deeds, mortgage documents, Forms 1098, receipts, bankruptcy filings and related papers, documents, schedules, correspondence, and payment records;

e. Address and/or telephone indices or books, calendars, records or notations reflecting names, addresses, telephone numbers, pager numbers, e-mail addresses, and fax numbers of financial institutions, mailbox and postal service business applications, addresses, proof of acquisition and/or expenditures, individuals, or businesses with whom a relationship exists;

f. United States currency, foreign currency, checks, money orders, cash of any kind or cash equivalents, jewelry, coins, and bullion.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review any information removed from the premises in order to locate the things particularly described in this Warrant.